AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

ORIGINAL

❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Seagate SATA hard disc drive, serial number 5VCEH45X, currently in secure evidence storage at the FBI, more fully described in Attachment A	)	Case No. 3:21-mc-1109

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Oregon

(identify the person or describe the property to be searched and give its location):

Seagate SATA hard disc drive, serial number 5VCEH45X, currently in secure evidence storage at the FBI, more fully described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before October 28, 2021 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge Youlee Yim You, via the Clerk .

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: October 14, 2021 5:16 p.m.

Youlee Yim You

Judge's signature

City and state: Portland, Oregon

Honorable Youlee Yim You, U.S. Magistrate Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:21-mc-1109	10-20-2021 at 1:10 pm	Heather Heck, FBI

Inventory made in the presence of :

Heather Heck, FBI

Inventory of the property taken and name(s) of any person(s) seized:

One Seagate SATA hard disc drive, serial number 5VCEH45X

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 10-22-2021

Cassandra Sommers

Executing officer's signature

Cassandra Sommers, Special Agent

Printed name and title

ATTACHMENT A

Item to be Searched

The following digital device, which was turned over to the FBI by Daniel Midget on August 12, 2021, and is currently in secure evidence storage at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland Oregon 97220:

Seagate SATA hard disc drive, serial number 5VCEH45X

ATTACHMENT B

Data to be Seized

1. All data on the device described in Attachment A ("the device") that relate to violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B) (transportation, receipt, distribution, and possession of child pornography), including:

a. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including digital images and video clips;

b. All images or video recordings that are self-produced and pertain to sexually explicit images of minors, or video recordings of minors that may assist in the location of minor victims of child exploitation or child abuse;

c. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

d. Evidence of Internet usage for the transportation, receipt, distribution, or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage, IP addresses, and any screen names, usernames, email addresses, or passwords used to access the Internet or any accounts via the Internet;

e. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means

(including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. All records or information referring or pertaining to communications with others for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, email communications, address books or contact list entries, and digital images sent or received;

h. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed.

2. Physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the device or its data.

3. Passwords, password files, test keys, encryption codes, or other information necessary to access the device or its data.

4. Evidence of user attribution showing who owned or used the device at the time the things described in this attachment were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, items and articles of identification, documents, and browsing history.

5. Records evidencing the use of the Internet, including:

a. Records of IP addresses used;

b. Records of Internet activity, including caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses; and

c. Records of online data storage accounts and use of data storage accounts.

6. As used above, the terms "records" and "information" include all items of evidence in whatever form and by whatever means they were created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

7. Because the device is already in law enforcement custody, it will be transported to a forensic laboratory for examination. The examination may require authorities to employ techniques, including computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

8. The initial examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If the government needs additional time to conduct this review, it may seek an extension of time from the Court within the original 120-day period from the date the warrant was executed. The government shall complete this review within 180 days of the date the warrant was executed. If the government needs additional time to complete this review, it may seek an extension of time from the Court.

9. If, at the conclusion of the examination, law enforcement personnel determine that specific files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

10. If an examination is conducted and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to the owner within a reasonable period following the search and will seal any image of the device, absent further authorization from the Court.

11. The government may retain the device if it contains contraband or evidence, if it constitutes fruits or an instrumentality of a crime, or to commence forfeiture proceedings against the device or its data.

12. The government will retain a forensic image of the device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.